Balík nástrojov Microsoft Sysinternals

Marek Čederle
xcederlem@stuba.sk

Fakulta informatiky a informačných technológií
Slovenská Technická Univerzita v Bratislave

02.12.2024

Obsah

Obsah

Microsoft Sysinternals

- Pôvodne `ntinternals` od spoločnosti Winternals Software
- Zakladatelia:
  - Mark Russinovich
  - Bryce Cogswell
- Spoločnosť Winternals Software bola v roku 2006 odkúpená spoločnosťou Microsoft
- Nástroje slúžiace pre pre správu, diagnostiku a monitorovanie systémov s OS Windows.

Zoznam nástrojov

Tabuľka č. 1: Zoznam nástrojov balíka Sysinternals

AccessChk	DiskView	**Process Explorer**	RegHide
AccessEnum	Disk Usage (DU)	**Process Monitor**	RegJump
AdExplorer	EFSDump	PsExec	Registry Usage (RU)
AdInsight	FindLinks	PsFile	SDelete
AdRestore	Handle	PsGetSid	ShareEnum
Autologon	Hex2dec	PsInfo	ShellRunas
Autoruns	Junction	PsKill	Sigcheck
BgInfo	LDMDump	PsList	Streams
BlueScreen	ListDLLs	PsLoggedOn	Strings
CacheSet	LiveKd	PsLogList	Sync
ClockRes	LoadOrder	PsPasswd	Sysmon
Contig	LogonSessions	PsPing	**TCPView**
Coreinfo	MoveFile	PsService	VMMap
Ctrl2Cap	NotMyFault	PsShutdown	VolumeID
DebugView	NTFSInfo	PsSuspend	WhoIs
Desktops	PendMoves	PsTools	WinObj
Disk2vhd	PipeList	RAMMap	ZoomIt
DiskExt	PortMon	RDCMan	—
DiskMon	ProcDump	RegDelNull	—

Microsoft Sysinternals

Vybrané nástroje

- Process Explorer
- Autoruns
- TCPView
- Process Monitor (ProcMon)

Prečo?

- Nástroje zamerané na:
  - bezpečnosť
  - analýzu správania procesov (malvéru)
  - diagnostiku systému
- Veľké množstvo nástrojov, mimo rozsah projektu

Obsah

Process Explorer

- Podobný ako Task Manager s pridanými/vylepšenými funkciami
- Nazývaný aj ako "Task Manager na steroidoch"
- Stromová štruktúra procesov (parent → child)

Pridané funkcie

- Dokáže zobraziť:
  - stack procesu/vlákna
  - DLL knižnice využívané procesom
  - sieťové spojenia procesu
- Odoslanie vzorky na VirusTotal.com
- Overenie signatúr
- Vyhľadávanie

Autoruns

- Správa programov spúšťaných pri štarte systému

Funkcie

- Odoslanie vzorky na VirusTotal.com
- Overenie signatúr

Tabuľka č. 2: Záložky nástroja Autoruns

Kategória	Popis
Logon	Programy spúšťané po prihlásení používateľa
Explorer	Rozšírenia a doplnky pre Windows Explorer
Scheduled Tasks	Úlohy spúšťané Plánovačom úloh
Services	Systémové služby spúšťané na pozadí
Drivers	Ovládače načítavané pri štarte systému

TCPView

- Monitorovanie sieťovej aktivity a spojení procesov
- Identifikácia nežiadúcich sieťových spojení
- Vylepšená GUI verzia CLI nástroja `netstat`
- Podporuje TCP/UDP, IPv4/IPv6
- Jednoduchší ako Wireshark – nezachytáva detaily packetov, iba aktívne spojenia

Process Monitor (ProcMon)

- Real-time monitorovanie operačného systému
- Diagnostika a riešenie problémov

Funkcie

- Filtrovanie udalostí
- Sledovanie krátko existujúcich procesov
- Zobrazuje veľa podrobných informácií o procesoch

When in doubt, run ProcMon!

— Mark Russinovich

Obsah

Príprava na experimentovanie

- Vytvorenie virtuálneho stroja na cloudovej platforme `Linode`
- Stiahnutie balíka nástrojov z oficiálnej stránky

Prečo nie lokálne?

- Vyššia bezpečnosť pri práci s malvérom
- Neinfikovanie lokálneho stroja

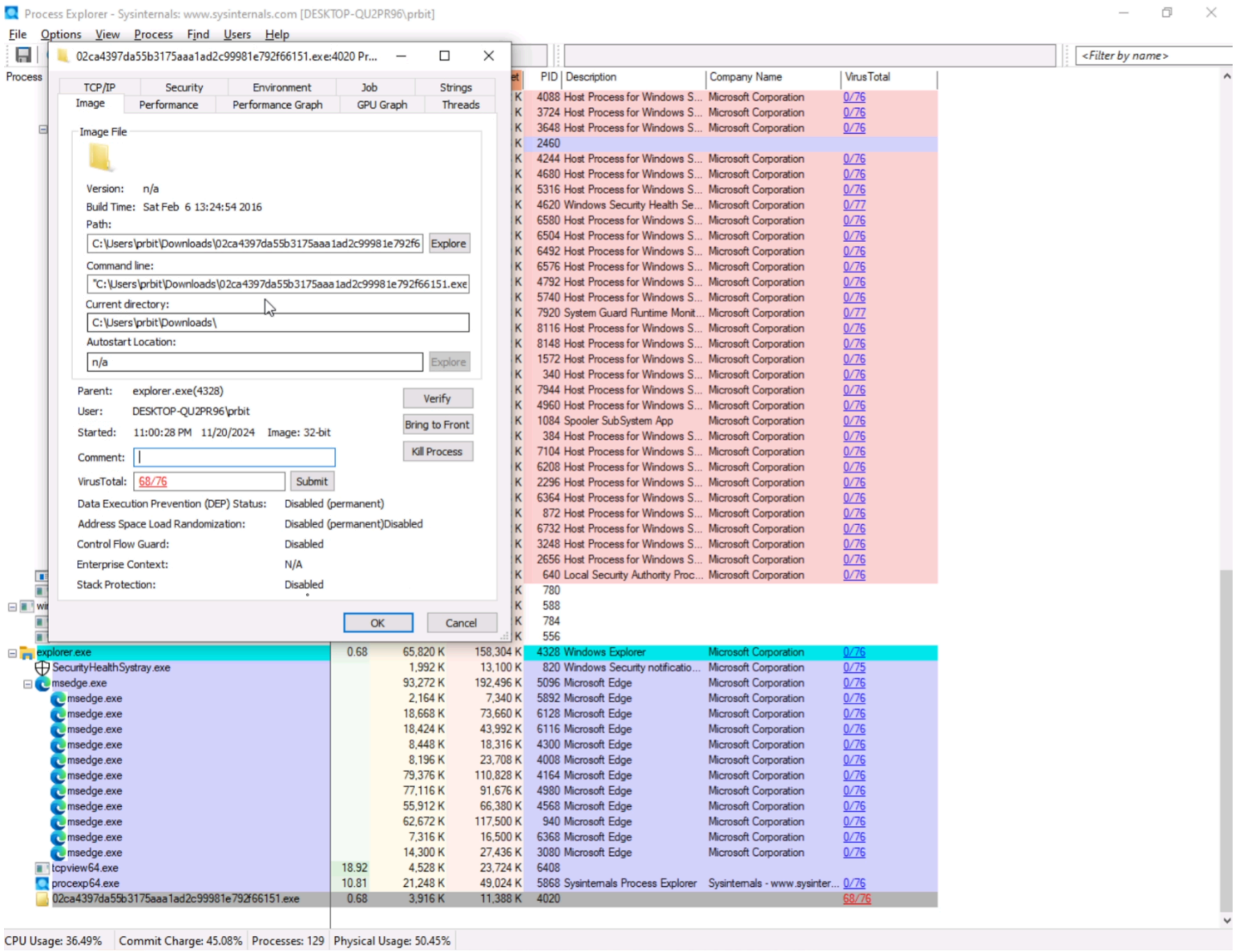
Experimenty

- Snažil som sa vybrať malvér na otestovanie funkcionality nástrojov
- Staršie vzorky malvéru (známe anti-malvér enginom)

Stiahnuté vzorky malvéru

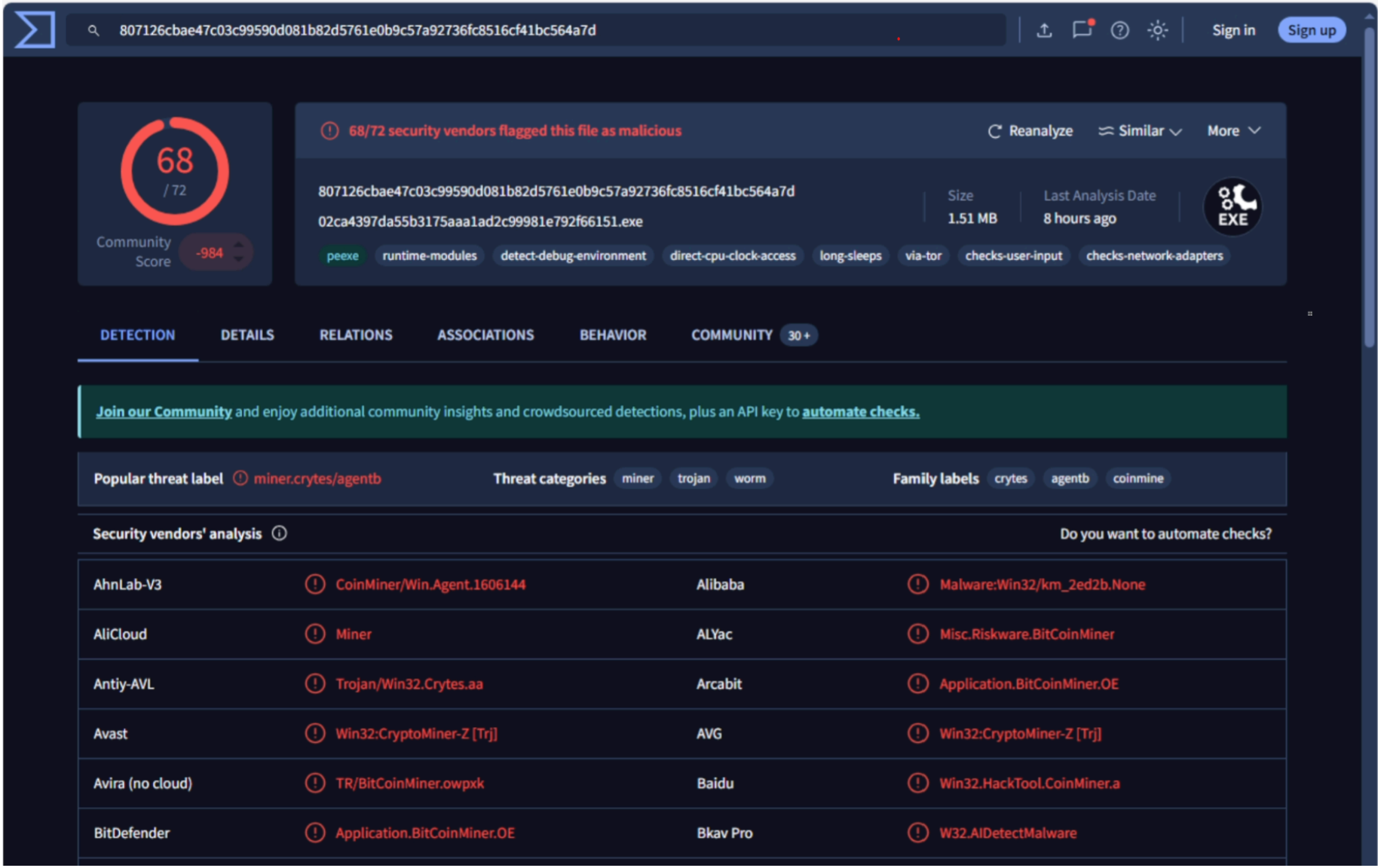
- Bitcoin Miner
- CryptBot
- Vidar Stealer
- DCRat — Dark Crystal RAT (Remote Access Trojan)

Malware sample 1: Bitcoin Miner



Obrázok č. 1: Bitcoin Miner — Process Explorer

Malware sample 1: Bitcoin Miner



Obrázok č. 2: Bitcoin Miner — VirusTotal.com

Malware sample 1: Bitcoin Miner

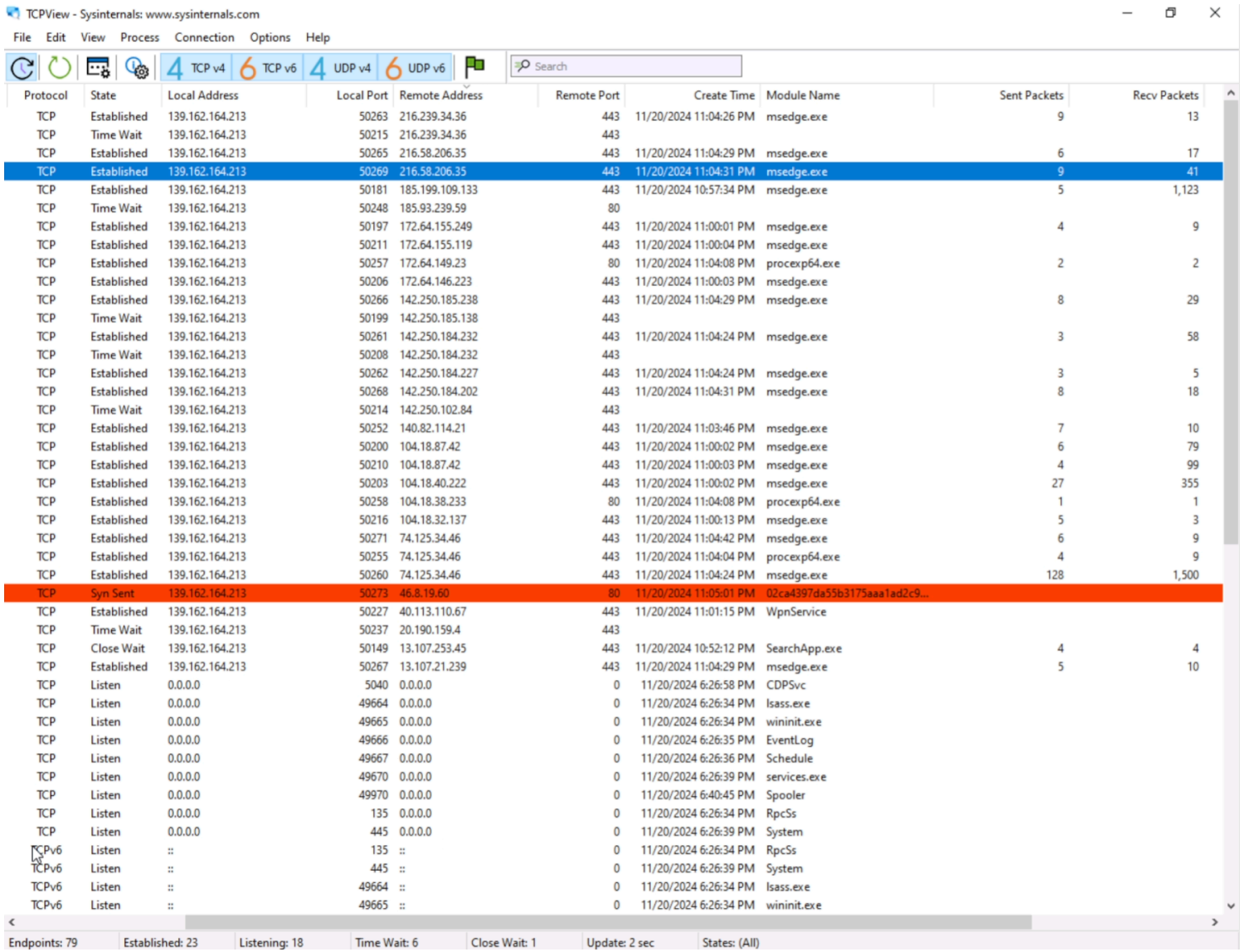
Autoruns

- Nenašla sa žiadna viditeľná aktivita
- Malvér pravdepodobne skrýval svoje správanie

TCPView

- Zachytené pokusy o pripojenie na vzdialené IP adresy
- Spojenia boli neúspešné (neaktívne IP adresy)

Malware sample 1: Bitcoin Miner



Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets
TCP	Established	139.162.164.213	50263	216.239.34.36	443	11/20/2024 11:04:26 PM	msedge.exe	9	13
TCP	Time Wait	139.162.164.213	50215	216.239.34.36	443				
TCP	Established	139.162.164.213	50265	216.58.206.35	443	11/20/2024 11:04:29 PM	msedge.exe	6	17
TCP	Established	139.162.164.213	50269	216.58.206.35	443	11/20/2024 11:04:31 PM	msedge.exe	9	41
TCP	Established	139.162.164.213	50181	185.199.109.133	443	11/20/2024 10:57:34 PM	msedge.exe	5	1,123
TCP	Time Wait	139.162.164.213	50248	185.93.239.59	80				
TCP	Established	139.162.164.213	50197	172.64.155.249	443	11/20/2024 11:00:01 PM	msedge.exe	4	9
TCP	Established	139.162.164.213	50211	172.64.155.119	443	11/20/2024 11:00:04 PM	msedge.exe		
TCP	Established	139.162.164.213	50257	172.64.149.23	80	11/20/2024 11:04:08 PM	procexp64.exe	2	2
TCP	Established	139.162.164.213	50206	172.64.146.223	443	11/20/2024 11:00:03 PM	msedge.exe		
TCP	Established	139.162.164.213	50266	142.250.185.238	443	11/20/2024 11:04:29 PM	msedge.exe	8	29
TCP	Time Wait	139.162.164.213	50199	142.250.185.138	443				
TCP	Established	139.162.164.213	50261	142.250.184.232	443	11/20/2024 11:04:24 PM	msedge.exe	3	58
TCP	Time Wait	139.162.164.213	50208	142.250.184.232	443				
TCP	Established	139.162.164.213	50262	142.250.184.227	443	11/20/2024 11:04:24 PM	msedge.exe	3	5
TCP	Established	139.162.164.213	50268	142.250.184.202	443	11/20/2024 11:04:31 PM	msedge.exe	8	18
TCP	Time Wait	139.162.164.213	50214	142.250.102.84	443				
TCP	Established	139.162.164.213	50252	140.82.114.21	443	11/20/2024 11:03:46 PM	msedge.exe	7	10
TCP	Established	139.162.164.213	50200	104.18.87.42	443	11/20/2024 11:00:02 PM	msedge.exe	6	79
TCP	Established	139.162.164.213	50210	104.18.87.42	443	11/20/2024 11:00:03 PM	msedge.exe	4	99
TCP	Established	139.162.164.213	50203	104.18.40.222	443	11/20/2024 11:00:02 PM	msedge.exe	27	355
TCP	Established	139.162.164.213	50258	104.18.38.233	80	11/20/2024 11:04:08 PM	procexp64.exe	1	1
TCP	Established	139.162.164.213	50216	104.18.32.137	443	11/20/2024 11:00:13 PM	msedge.exe	5	3
TCP	Established	139.162.164.213	50271	74.125.34.46	443	11/20/2024 11:04:42 PM	msedge.exe	6	9
TCP	Established	139.162.164.213	50255	74.125.34.46	443	11/20/2024 11:04:04 PM	procexp64.exe	4	9
TCP	Established	139.162.164.213	50260	74.125.34.46	443	11/20/2024 11:04:24 PM	msedge.exe	128	1,500
TCP	Syn Sent	139.162.164.213	50273	46.8.19.60	80	11/20/2024 11:05:01 PM	02ca4397da55b3175aaa1ad2c9...		
TCP	Established	139.162.164.213	50227	40.113.110.67	443	11/20/2024 11:01:15 PM	WpnService		
TCP	Time Wait	139.162.164.213	50237	20.190.159.4	443				
TCP	Close Wait	139.162.164.213	50149	13.107.253.45	443	11/20/2024 10:52:12 PM	SearchApp.exe	4	4
TCP	Established	139.162.164.213	50267	13.107.21.239	443	11/20/2024 11:04:29 PM	msedge.exe	5	10
TCP	Listen	0.0.0.0	5040	0.0.0.0	0	11/20/2024 6:26:58 PM	CDPSvc		
TCP	Listen	0.0.0.0	49664	0.0.0.0	0	11/20/2024 6:26:34 PM	lsass.exe		
TCP	Listen	0.0.0.0	49665	0.0.0.0	0	11/20/2024 6:26:34 PM	wininit.exe		
TCP	Listen	0.0.0.0	49666	0.0.0.0	0	11/20/2024 6:26:35 PM	EventLog		
TCP	Listen	0.0.0.0	49667	0.0.0.0	0	11/20/2024 6:26:36 PM	Schedule		
TCP	Listen	0.0.0.0	49670	0.0.0.0	0	11/20/2024 6:26:39 PM	services.exe		
TCP	Listen	0.0.0.0	49970	0.0.0.0	0	11/20/2024 6:40:45 PM	Spooler		
TCP	Listen	0.0.0.0	135	0.0.0.0	0	11/20/2024 6:26:34 PM	RpcSs		
TCP	Listen	0.0.0.0	445	0.0.0.0	0	11/20/2024 6:26:39 PM	System		
TCPv6	Listen	::	135	::	0	11/20/2024 6:26:34 PM	RpcSs		
TCPv6	Listen	::	445	::	0	11/20/2024 6:26:39 PM	System		
TCPv6	Listen	::	49664	::	0	11/20/2024 6:26:34 PM	lsass.exe		
TCPv6	Listen	::	49665	::	0	11/20/2024 6:26:34 PM	wininit.exe		

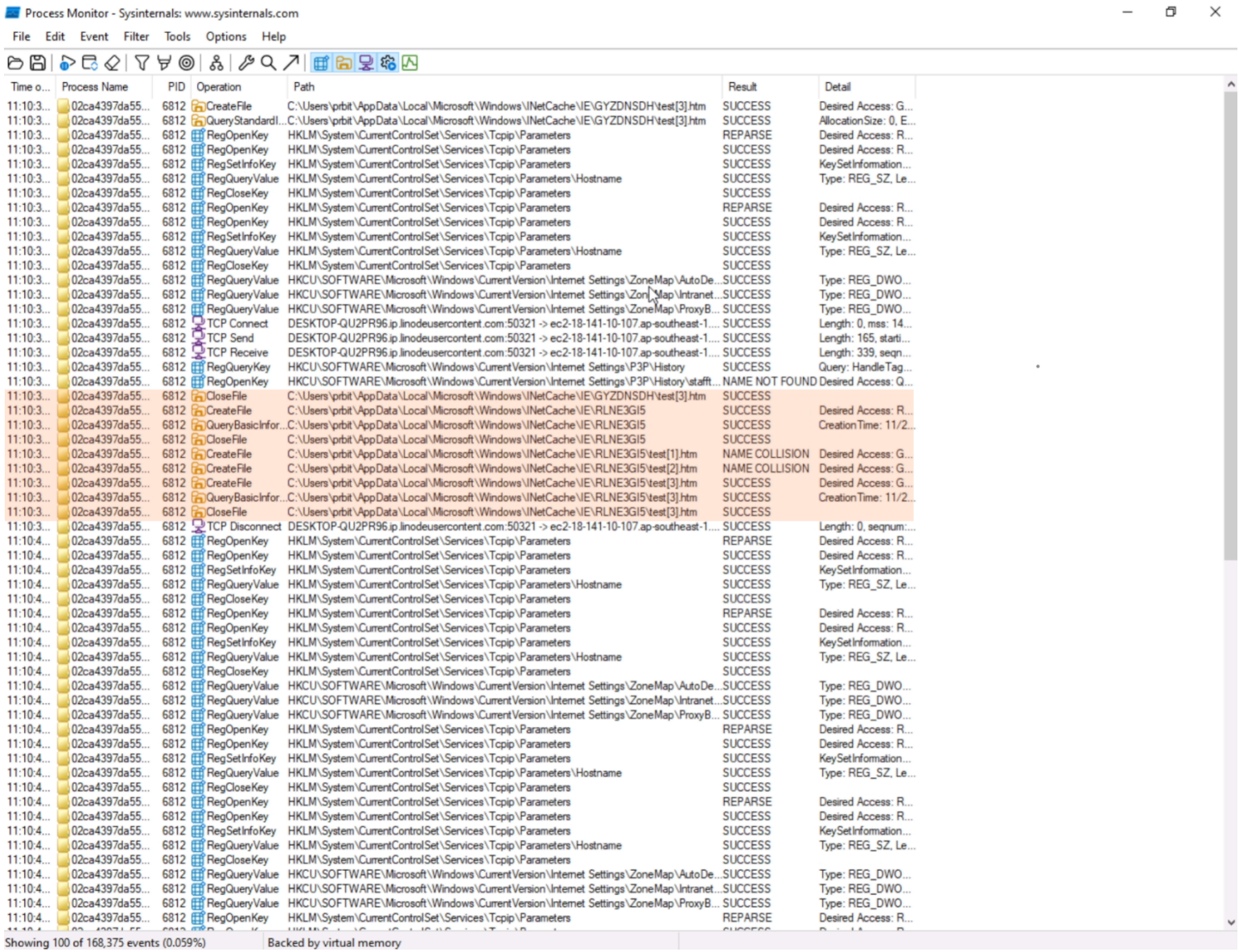
Obrázok č. 3: Bitcoin Miner — TCPView

Malware sample 1: Bitcoin Miner

Process Monitor (ProcMon)

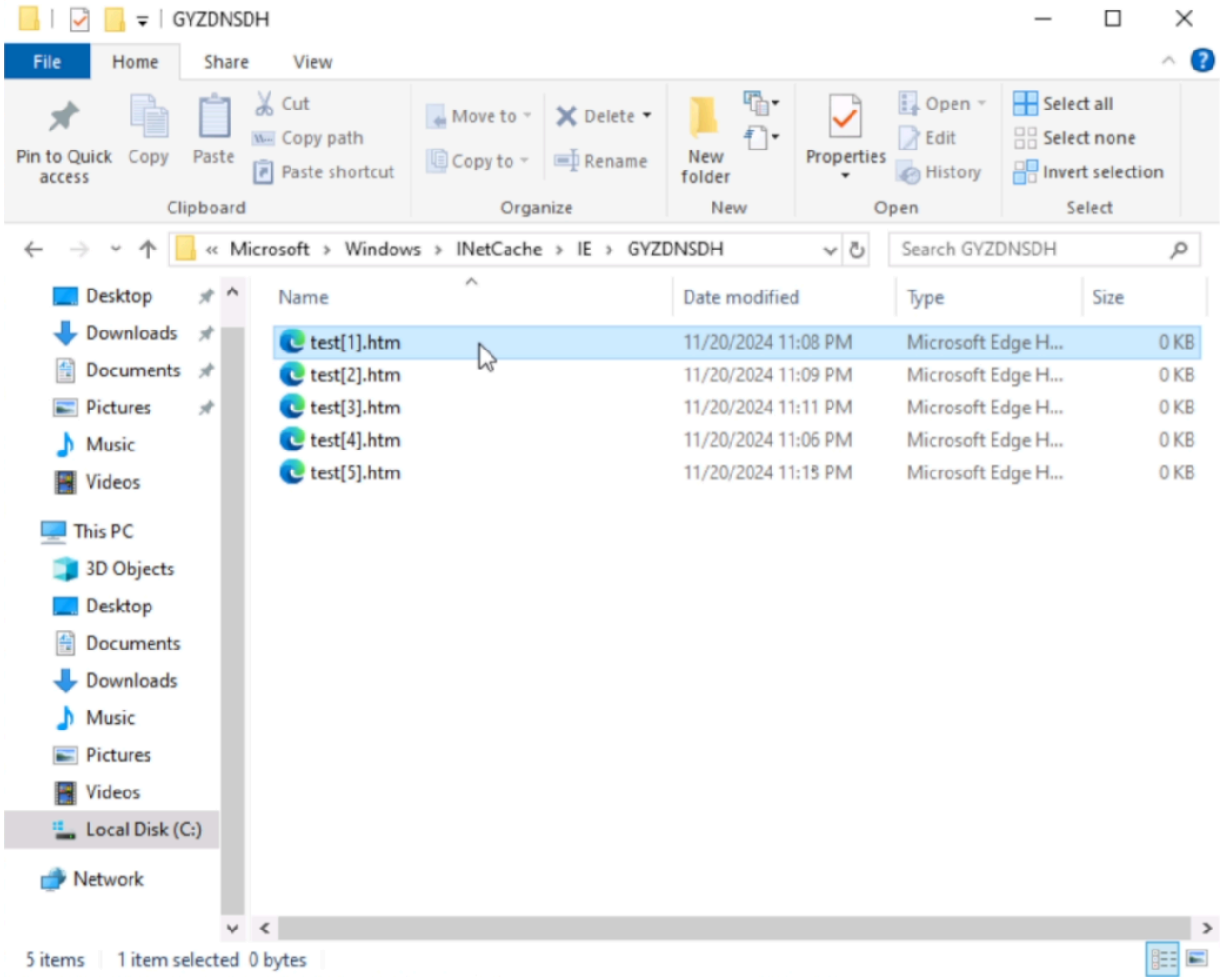
- Zachytené aktivity:
  - Prístup ku kľúčom registrov
  - Vytváranie sieťových spojení
  - Vytváranie (prázdnych `.htm`) súborov

Malware sample 1: Bitcoin Miner



Obrázok č. 4: Bitcoin Miner — Process Monitor

Malware sample 1: Bitcoin Miner



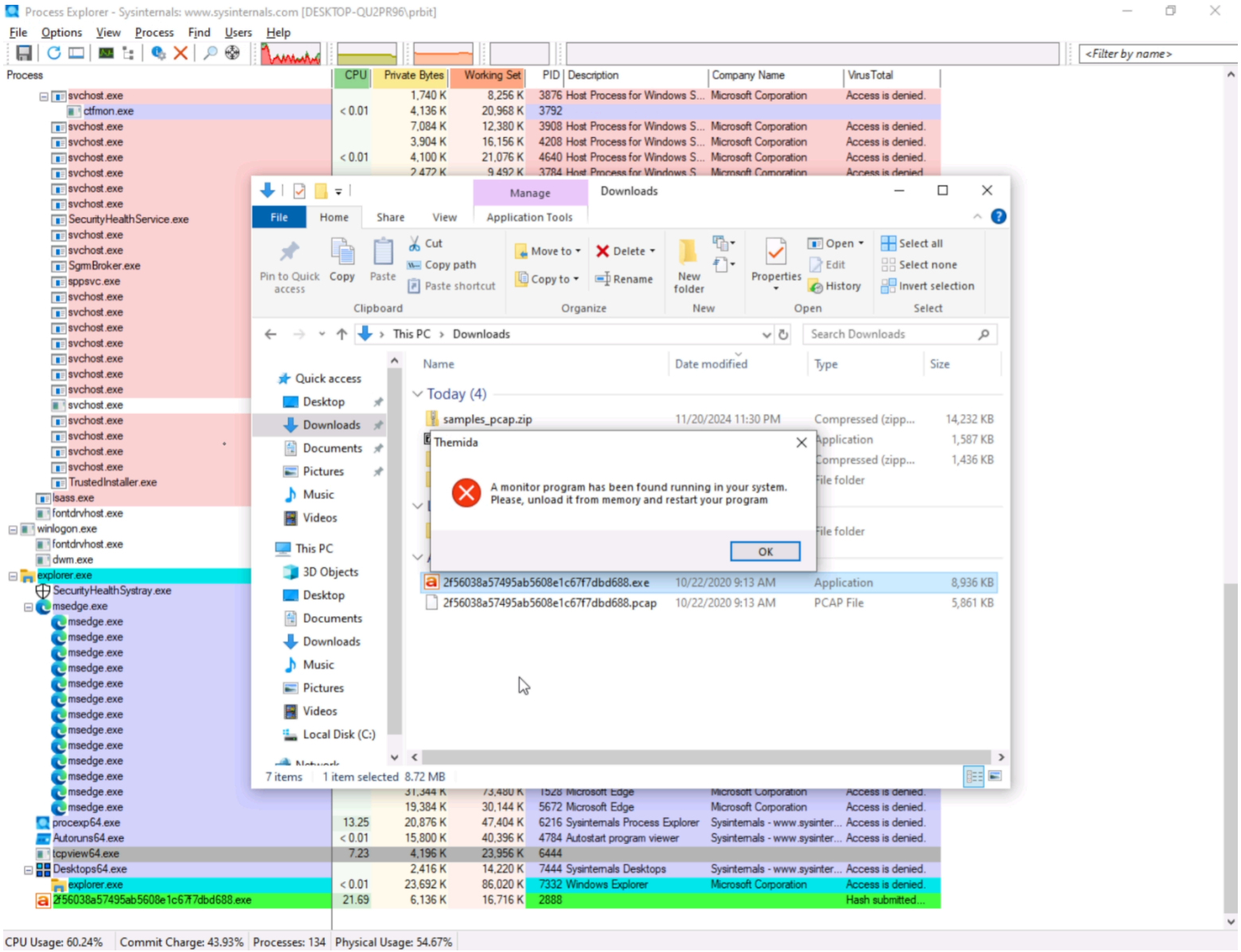
Obrázok č. 5: Bitcoin Miner — Náhodné súbory

Malware sample 2: CryptBot

CryptBot

- Sofistikovaný malvér
- Deteguje nástroje ako Process Explorer alebo ProcMon
- Po vypnutí nástrojov sa stále odmietal spustiť

Malware sample 2: CryptBot



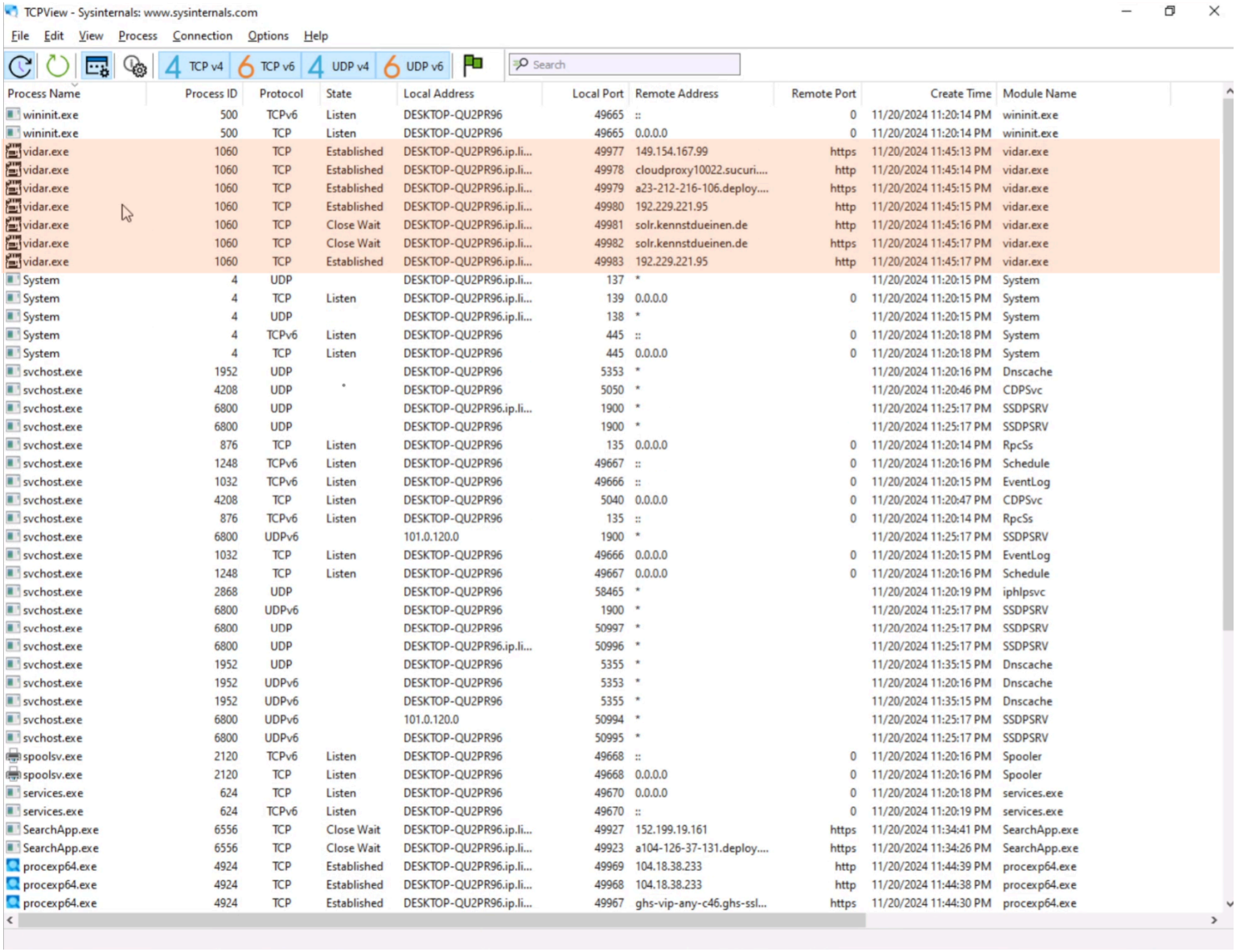
Obrázok č. 6: CryptBot — Chybová hláška

Malware sample 3: Vidar Stealer

Vidar Stealer

- Process Explorer taktiež ukázal veľa detekcií z anti-malvér enginov
- Malvér sa snažil odoslať údaje na vzdialené IP adresy
- Autoruns nám zasa nič nezobrazil
- Process Monitor odhalil interakciu s kľúčmi registrov súvisiacimi s webovým prehliadačom

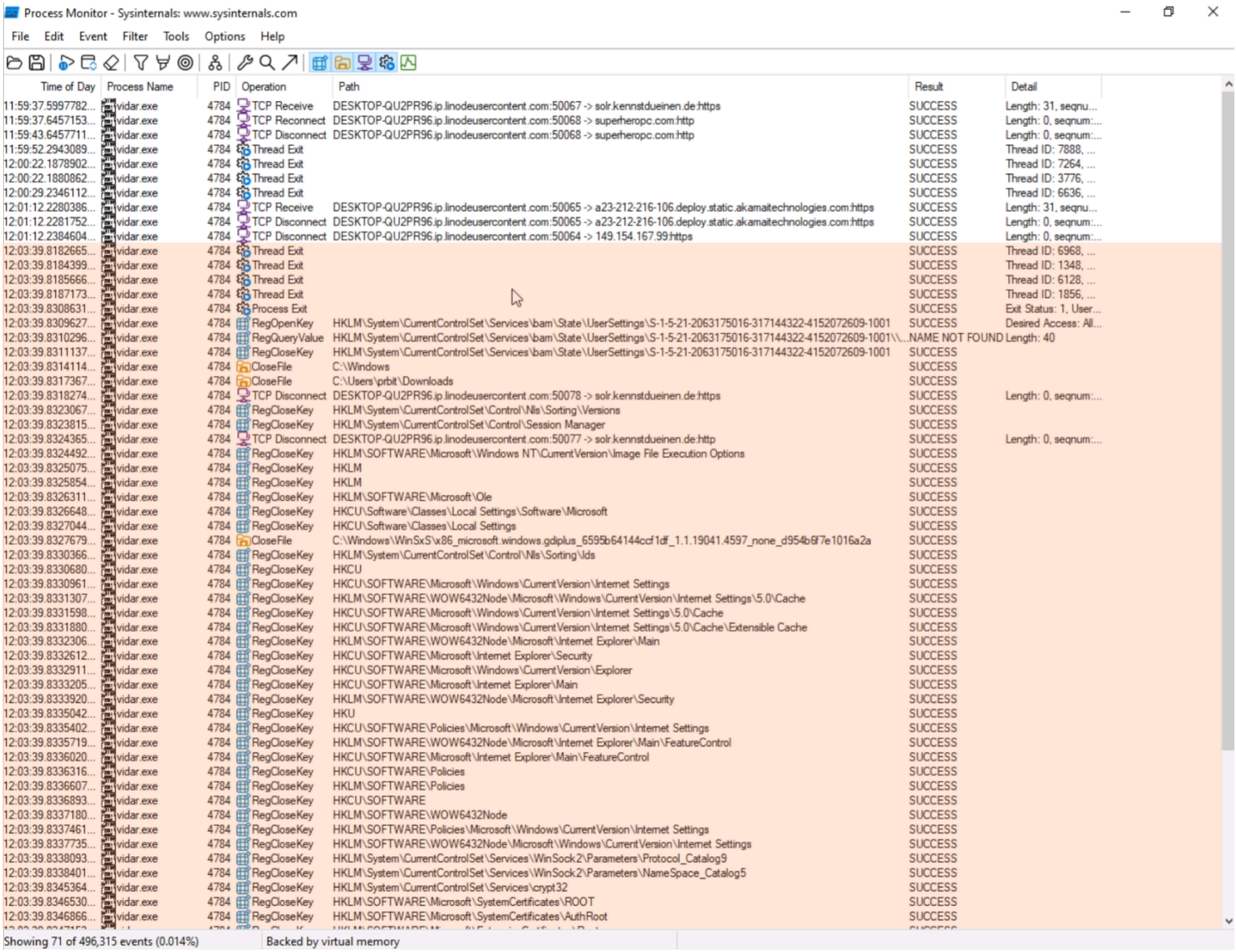
Malware sample 3: Vidar Stealer



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
wininit.exe	500	TCPv6	Listen	DESKTOP-QU2PR96	49665	::	0	11/20/2024 11:20:14 PM	wininit.exe
wininit.exe	500	TCP	Listen	DESKTOP-QU2PR96	49665	0.0.0.0	0	11/20/2024 11:20:14 PM	wininit.exe
vidar.exe	1060	TCP	Established	DESKTOP-QU2PR96.ip.li...	49977	149.154.167.99	https	11/20/2024 11:45:13 PM	vidar.exe
vidar.exe	1060	TCP	Established	DESKTOP-QU2PR96.ip.li...	49978	cloudproxy10022.sucuri....	http	11/20/2024 11:45:14 PM	vidar.exe
vidar.exe	1060	TCP	Established	DESKTOP-QU2PR96.ip.li...	49979	a23-212-216-106.deploy....	https	11/20/2024 11:45:15 PM	vidar.exe
vidar.exe	1060	TCP	Established	DESKTOP-QU2PR96.ip.li...	49980	192.229.221.95	http	11/20/2024 11:45:15 PM	vidar.exe
vidar.exe	1060	TCP	Close Wait	DESKTOP-QU2PR96.ip.li...	49981	solr.kennstdueinen.de	http	11/20/2024 11:45:16 PM	vidar.exe
vidar.exe	1060	TCP	Close Wait	DESKTOP-QU2PR96.ip.li...	49982	solr.kennstdueinen.de	https	11/20/2024 11:45:17 PM	vidar.exe
vidar.exe	1060	TCP	Established	DESKTOP-QU2PR96.ip.li...	49983	192.229.221.95	http	11/20/2024 11:45:17 PM	vidar.exe
System	4	UDP		DESKTOP-QU2PR96.ip.li...	137	*		11/20/2024 11:20:15 PM	System
System	4	TCP	Listen	DESKTOP-QU2PR96.ip.li...	139	0.0.0.0	0	11/20/2024 11:20:15 PM	System
System	4	UDP		DESKTOP-QU2PR96.ip.li...	138	*		11/20/2024 11:20:15 PM	System
System	4	TCPv6	Listen	DESKTOP-QU2PR96	445	::	0	11/20/2024 11:20:18 PM	System
System	4	TCP	Listen	DESKTOP-QU2PR96	445	0.0.0.0	0	11/20/2024 11:20:18 PM	System
svchost.exe	1952	UDP		DESKTOP-QU2PR96	5353	*		11/20/2024 11:20:16 PM	Dnscache
svchost.exe	4208	UDP		DESKTOP-QU2PR96	5050	*		11/20/2024 11:20:46 PM	CDPSvc
svchost.exe	6800	UDP		DESKTOP-QU2PR96.ip.li...	1900	*		11/20/2024 11:25:17 PM	SSDPSRV
svchost.exe	6800	UDP		DESKTOP-QU2PR96	1900	*		11/20/2024 11:25:17 PM	SSDPSRV
svchost.exe	876	TCP	Listen	DESKTOP-QU2PR96	135	0.0.0.0	0	11/20/2024 11:20:14 PM	RpcSs
svchost.exe	1248	TCPv6	Listen	DESKTOP-QU2PR96	49667	::	0	11/20/2024 11:20:16 PM	Schedule
svchost.exe	1032	TCPv6	Listen	DESKTOP-QU2PR96	49666	::	0	11/20/2024 11:20:15 PM	EventLog
svchost.exe	4208	TCP	Listen	DESKTOP-QU2PR96	5040	0.0.0.0	0	11/20/2024 11:20:47 PM	CDPSvc
svchost.exe	876	TCPv6	Listen	DESKTOP-QU2PR96	135	::	0	11/20/2024 11:20:14 PM	RpcSs
svchost.exe	6800	UDPv6		101.0.120.0	1900	*		11/20/2024 11:25:17 PM	SSDPSRV
svchost.exe	1032	TCP	Listen	DESKTOP-QU2PR96	49666	0.0.0.0	0	11/20/2024 11:20:15 PM	EventLog
svchost.exe	1248	TCP	Listen	DESKTOP-QU2PR96	49667	0.0.0.0	0	11/20/2024 11:20:16 PM	Schedule
svchost.exe	2868	UDP		DESKTOP-QU2PR96	58465	*		11/20/2024 11:20:19 PM	iphlpsvc
svchost.exe	6800	UDPv6		DESKTOP-QU2PR96	1900	*		11/20/2024 11:25:17 PM	SSDPSRV
svchost.exe	6800	UDP		DESKTOP-QU2PR96	50997	*		11/20/2024 11:25:17 PM	SSDPSRV
svchost.exe	6800	UDP		DESKTOP-QU2PR96.ip.li...	50996	*		11/20/2024 11:25:17 PM	SSDPSRV
svchost.exe	1952	UDP		DESKTOP-QU2PR96	5355	*		11/20/2024 11:35:15 PM	Dnscache
svchost.exe	1952	UDPv6		DESKTOP-QU2PR96	5353	*		11/20/2024 11:20:16 PM	Dnscache
svchost.exe	1952	UDPv6		DESKTOP-QU2PR96	5355	*		11/20/2024 11:35:15 PM	Dnscache
svchost.exe	6800	UDPv6		101.0.120.0	50994	*		11/20/2024 11:25:17 PM	SSDPSRV
svchost.exe	6800	UDPv6		DESKTOP-QU2PR96	50995	*		11/20/2024 11:25:17 PM	SSDPSRV
spoolsv.exe	2120	TCPv6	Listen	DESKTOP-QU2PR96	49668	::	0	11/20/2024 11:20:16 PM	Spooler
spoolsv.exe	2120	TCP	Listen	DESKTOP-QU2PR96	49668	0.0.0.0	0	11/20/2024 11:20:16 PM	Spooler
services.exe	624	TCP	Listen	DESKTOP-QU2PR96	49670	0.0.0.0	0	11/20/2024 11:20:18 PM	services.exe
services.exe	624	TCPv6	Listen	DESKTOP-QU2PR96	49670	::	0	11/20/2024 11:20:19 PM	services.exe
SearchApp.exe	6556	TCP	Close Wait	DESKTOP-QU2PR96.ip.li...	49927	152.199.19.161	https	11/20/2024 11:34:41 PM	SearchApp.exe
SearchApp.exe	6556	TCP	Close Wait	DESKTOP-QU2PR96.ip.li...	49923	a104-126-37-131.deploy....	https	11/20/2024 11:34:26 PM	SearchApp.exe
procexp64.exe	4924	TCP	Established	DESKTOP-QU2PR96.ip.li...	49969	104.18.38.233	http	11/20/2024 11:44:39 PM	procexp64.exe
procexp64.exe	4924	TCP	Established	DESKTOP-QU2PR96.ip.li...	49968	104.18.38.233	http	11/20/2024 11:44:38 PM	procexp64.exe
procexp64.exe	4924	TCP	Established	DESKTOP-QU2PR96.ip.li...	49967	ghs-vip-any-c46.ghs-ssl...	https	11/20/2024 11:44:30 PM	procexp64.exe

Obrázok č. 7: Vidar Stealer — TCPView

Malware sample 3: Vidar Stealer



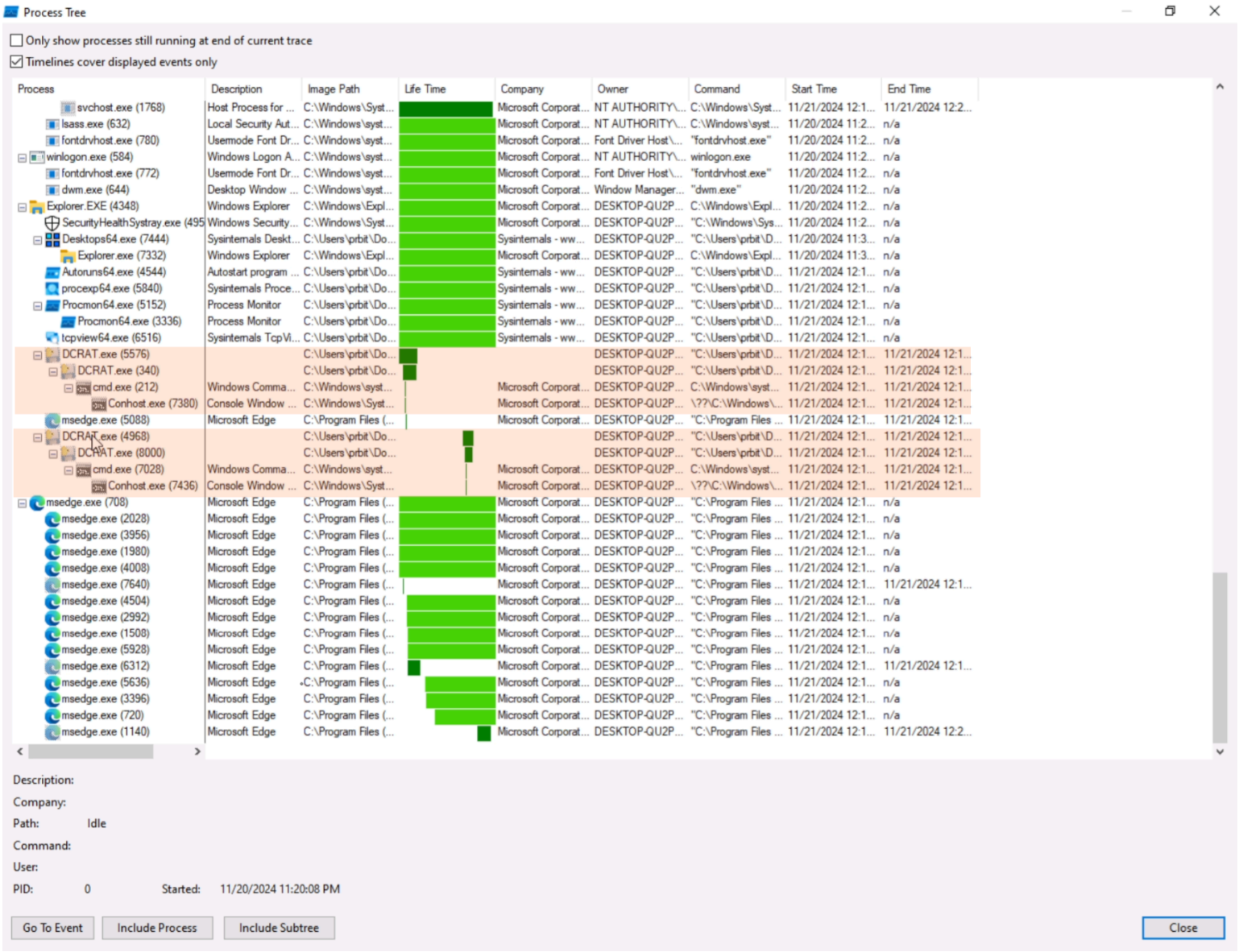
Obrázok č. 8: Vidar Stealer — Process Monitor

Malware sample 4: DCRat

DCRat

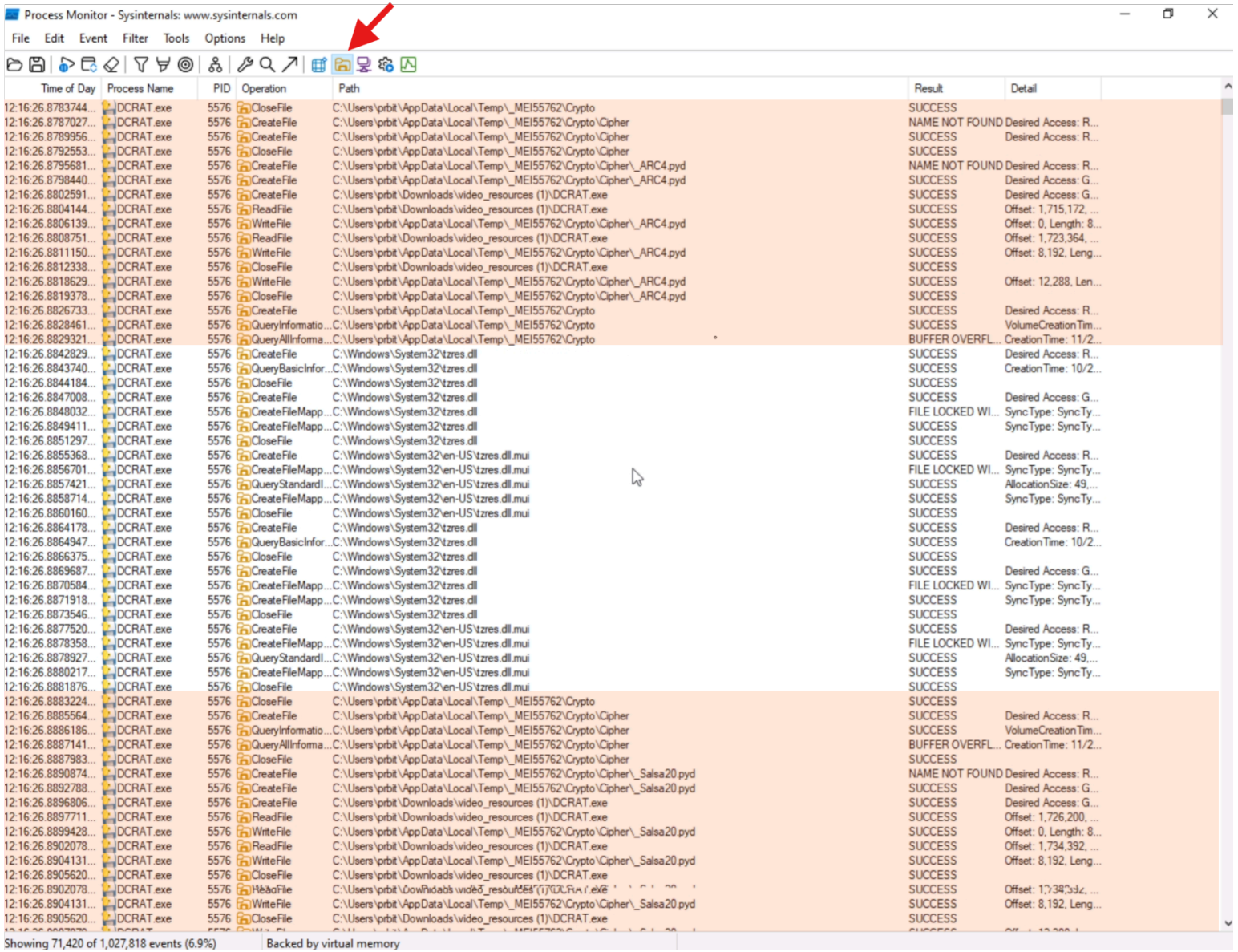
- VirusTotal opäť identifikoval proces ako malvér
- Autoruns opäť neukázal žiadne záznamy (týkajúce sa malvéru)
- TCPView potvrdil pripojenie na vzidalené IP adresy
- Process Monitor odhalil viacero sub-procesov, ktoré sa po chvíli ukončili a pokusy o operácie nad súbormi

Malware sample 4: DCRat



Obrázok č. 9: DCRat — Process Monitor

Malware sample 4: DCRat



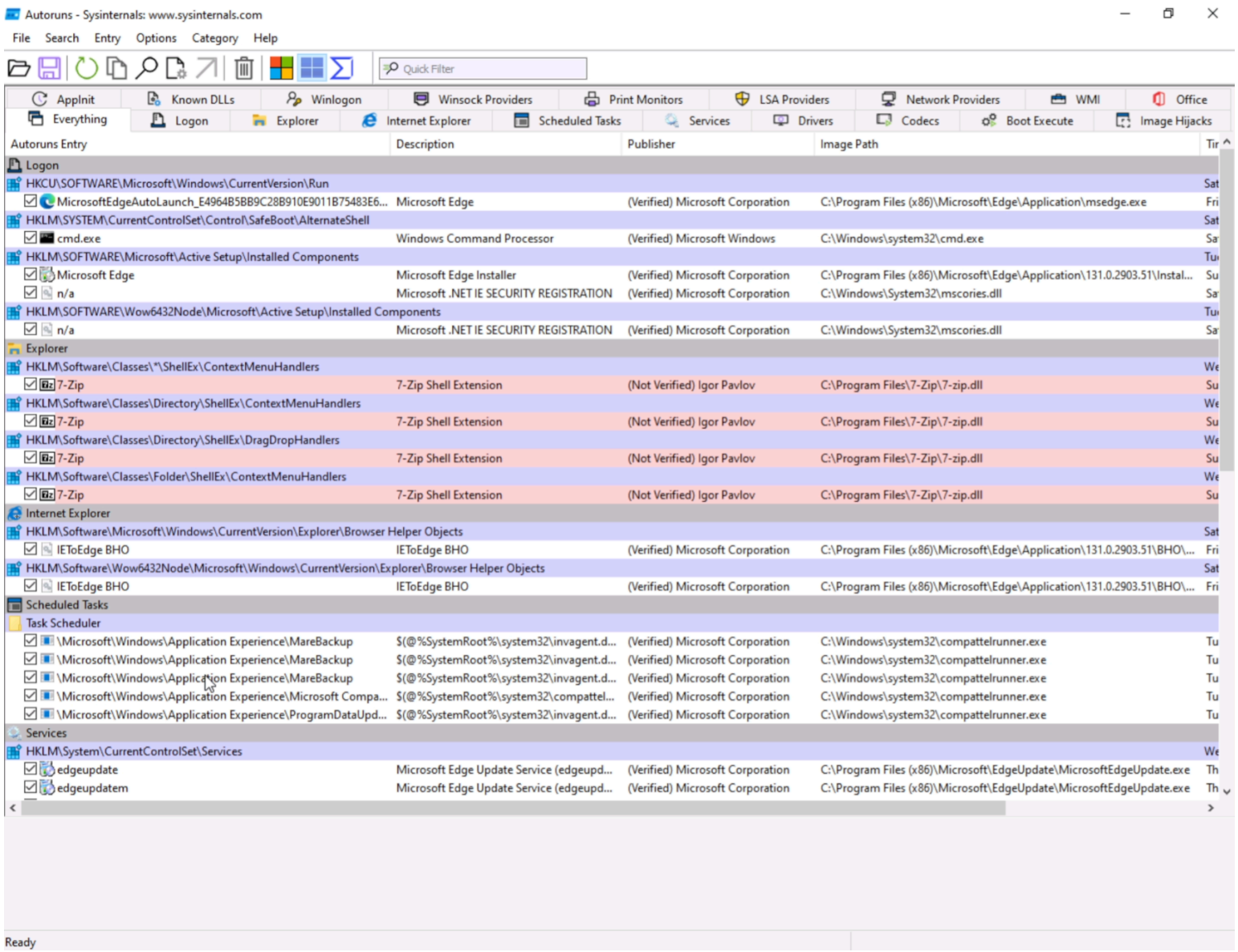
Obrázok č. 10: DCRat — Operácie so súbormi

Experiment s legitímnym softvérom

Autoruns — 7-zip

- Legitímny softvér `7-zip` má neoverený certifikát (vývojár neplatí Microsoftu za licenciu)
- VirusTotal vrátil 0 detekcií
- Softvér sa zapísal do viacero kľúčov registrov

Experiment s legitímnym softvérom



Obrázok č. 11: Autoruns — Ukážka pre legitímny softvér

Obsah

Zhodnotenie

Výhody

- Veľmi užitočné nástroje pre detekciu a analýzu správania malvéru
- Užitočné pre bezpečnostných expertov, IT technikov

Nevýhody

- Pokročilé malvéry sa vyhýbajú detekcii
- Obyčajný používatelia sa môžu v nástrojoch stratiť

Ďakujem za pozornosť!

Literatúra

[1] Wikipedia contributors, "Sysinternals — Wikipedia, The Free Encyclopedia." [Online]. Available: https://en.wikipedia.org/w/index.php?title=Sysinternals&oldid=1248667707

[2] Microsoft, "Microsoft Sysinternals Documentation." [Online]. Available: https://learn.microsoft.com/en-us/sysinternals/

[3] VirusTotal contributors, "VirusTotal Documentation Hub." [Online]. Available: https://docs.virustotal.com/

[4] Scott Lott, "Installing Windows on a Linode VPS." [Online]. Available: https://github.com/only-cliches/docs/blob/windows-on-linode/docs/tools-reference/windows-on-linode/installing-windows-on-linode-vps.md

[5] Mark Russinovich, "License to Kill: Malware Hunting with the Sysinternals Tools." [Online]. Available: https://www.youtube.com/watch?v=A_TPZxuTzBU

Literatúra

[6] Windows IT Pro, "Sysinternals Overview | Microsoft, tools, utilities, demos." [Online]. Available: https://www.youtube.com/watch?v=6RqFPrCcWfY

[7] Fabrizio Monaco, "Malware Samples Repository." [Online]. Available: https://github.com/fabrimagic72/malware-samples/tree/master

[8] Josh Stroschein, "Malware Samples Repository." [Online]. Available: https://github.com/jstrosch/malware-samples